## REMARKS

In response to the Office Action mailed July 2, 2007, Applicant respectfully requests reconsideration. Claims 1-23 were previously pending in this application. By this amendment, Claims 2, 5, 10, 12, 15 and 18 have been amended. As a result, claims 1-23 are pending for examination with claims 1, 8, 15, 18 and 20 being independent claims. No new matter has been added.

### Rejections Under 35 U.S.C. §102

Claims 1-2, 4, 6-9, 11, and 13-17 are rejected under 35 U.S.C. 102(e)as being anticipated by Balissat, et al., U.S. Patent No. 7,188,365. Applicants respectfully disagree.

The present application describes a method of authenticating devices communicating over a network that can be implemented as an extension to existing protocols, such as the Internet Key Management (IKE) protocol (paragraph 33) used in establishing an IPsec security association. Accordingly, there are similarities between the present application and the references, which also describe those existing protocols. However, Applicants respectfully submit that the extension to those existing protocols described in the present application is not shown or suggested in the references.

Specifically, the present application describes using a public key, used for encrypting information exchanged between a first device and a second device in accordance with the existing protocol, to also establish the authenticity of one of the devices. As described in the application, when the second device receives a public key from the first device, the second device determines whether the key matches the key of a known device. If so, when the second device successfully decrypts a message from a previously unauthenticated device using a shared secret created using that public key, the second device concludes that the message was in fact sent by the known device (see blocks 516, 616 in Fig. 5 and 6).

In contrast, Balissat describes a conventional approach of  using three sets of messages, with one set of messages exchanging keys and a subsequent exchange for authenticating the devices (col. 8, lines 12-20). Consequently, the reference does not teach or suggest all features of the claims.

As to independent claim 1, the claim recites that public keys are exchanged between devices and used for creating a shared secret for encrypting a payload. The claim further recites that "the shared secret is used to authenticate the identity of the responder" or "the shared secret is used to authenticate the identity of the initiator." The process of Balissat in which a separate set of messages is used for authentication does not teach or suggest a method as in claim 1.

Independent claim 8 recites that "the shared secret is used to authenticate the identity of the responder" or "the shared secret is used to authenticate the identity of the initiator," neither of which is shown or suggested in Balissat.

Independent claim 15 recites that "a static Diffie-Hellman (DH) key-pair is used...to establish confidentiality" and that "decryption of a message encrypted with the static Diffie-Hellman key-pair authenticates a device associated with the static key-pair." As noted above, Balissat does not teach or suggest that decryption of a message also authenticates the sender of the message.

Independent claim 20 recites that "the shared secret is used to authenticate the identity of the responder" or "the shared secret is used to authenticate the identity of the initiator," neither of which is shown or suggested in Balissat.

Claims 2-7, 9-14, 16-17 and 21-23 depend, directly or indirectly, from one of the independent claims discussed above and distinguishes the references for at least the same reasons. The dependent claims recite additional limitations that provide further reasons for patentability. For example, claim 4 recites: "the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator." Such a limitation further distinguishes systems using an ephemeral key pair to establish a security association because a device would not previously know an ephemeral key.

Accordingly, withdrawal of this rejection is respectfully requested.

## Rejections Under 35 U.S.C. §103

Claims 3, 5, 10, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balissat, et al. (US 7,188,365), and further in view of Daly, et al. (US 5,930,362). Claims 18 and 19 are also rejected based on the same combination of references. Applicants respectfully disagree with the rejections.

Claims 3, 5, 10, and 12 depend from one of the independent claims discussed above. As noted in connection with the discussion of the independent claims, Balissat does not teach or suggest using a key exchange for establishing a shared secret to encrypt messages between devices and to also authenticate at least one of the devices. Daly does not teach or suggest such a use of exchanged keys, either. Rather, Daly is cited to show that verification techniques could be implemented in mobile devices. Therefore, even if Daly were combined with Balissat, the combination would not teach or suggest all limitations of claims 3, 5, 10, and 12.

As a further distinguishing feature, the claims have been amended to indicate that the portable media device is separate from the devices that are communicating. Thus, Daly does not teach the asserted limitation of the claims as amended, providing an additional reason that the claims distinguish the references.

As to independent claim 18, the claim also recites details not shown or suggested in the references. The claim recites that the portable media device is separate from the second device, and therefore distinguishes Daly. In addition, the claim recites "using the public key of the DH key pair to ensure confidentiality and authenticity in securing a communications channel with another networked device, following the Internet Key Exchange (IKE) and Internet Security (IPSec) protocols." The claim therefore distinguishes Balissat. In summary, even if the references were combined, they would not teach or suggest all limitations of claim 18.

Accordingly, withdrawal of this rejection is respectfully requested.

## CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: October 2, 2007

Respectfully submitted,

By: /Edmund J. Walsh/
Edmund J. Walsh
Registration No. 32,950
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000